UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,649	06/05/2001	Steven H. McCown	2001-025-SFT	5080

7590 05/04/2006

Wayne P. Bailey
Storage Technology Corporation
One StorageTek Drive
Louisville, CO 80028-4309

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/874,649
Filing Date: June 05, 2001
Appellant(s): MCCOWN ET AL.

Lisa L.B. Yociss
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02/13/2006 from the Office action mailed 09/12/2005.

Real Party in Interest

(1) A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences, which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

A statement of the status of the claims is contained in the brief.

(4) Status of Amendments after Final

A statement identifying the status of amendments after Final is contained in the brief.

(5) Summary of Claimed Subject Matter

The summary of invention contained in the brief is correct.

(6) Grouping of Claims

A statement identifying the grouping of claims is contained in the brief.

(7) Claims Appealed

A copy of appealed claims 1-3, 5-14, 16-21, 23-33 and 35-50 appears on pages 17-25 of the appellant's claim Appendix.

(8) Evidence

A statement identifying additional evidence is contained in the appellant's page 26 of the brief.*)*

(9) Prior Art of Record

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal:

Davis (US 6,292,892 B1)

(10) Grounds of Rejection to be reviewed on Appeal

The following ground(s) of rejection are applicable to the appealed claims:

A) The rejection of claims 1-3, 5-14, 16-21, 23-33 and 35-50 under U.S.C. § 112 first-paragraph is maintained (please see the related rejections below).

B) The New ground of Rejection with respect to the claims 1-3, 5-14, 16-21, 23-33 and 35-50 have been rendered in harmony with the U.S.C. § 112 first-paragraph rejections of the claims.

Claim Rejections - 35 USC § 112

1. **Claims 1, 13, 19, 31, 42 and 44** are rejected **under 35 U.S.C. 112, first paragraph**, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The limitation "the client being incapable of decrypting the encrypted data" has no support in the specification. Specification clearly discloses different

method of encrypting data and decryption the encrypted data. Nowhere on pages 11-16 disclose any support for the above limitation.

2. Dependent claims 2, 3, 5-12, 14, 16-18, 20, 21, 23-30, 32, 33, 35-41, 43 and 45-50 are rejected based on their dependency on the above rejected independent claims.

Claim Rejections - 35 USC § 102

3. **Claims 1-3, 5-14, 16-21, 23-33 and 35-50** are rejected under 35 U.S.C. 102(b) as being anticipated by Davis (6,292,892 B1).

As per claims 1 and 19 Davis (6,292,892 B1) teach a computer program product in a computer-readable medium for transmitting data in a network, a method of transmitting data in a network (see fig.1-3 and associated text such as col.1, lines 34-45 disclose medium for transmitting data back and forth between parties connected in a network environment; col.2, lines 60-67; col.3, lines 1-9 also disclose using a computer readable medium product such as CD may employed for such transmission of data) comprising: receiving from a client a request to transmit the data (see col.5, lines 66-67; col.6, lines 1-2 wherein the remote system random challenge transmission to the local system corresponds to applicant's client request for transmitting data for authentication reasons); encrypting the data (see col.6, lines 2-4 wherein the hardware agent within or associated with local system encrypts the challenge that corresponds to applicant's

"encrypting the data"); and transmitting the encrypted data to a storage device (see col.6, lines 4-5 wherein the encrypted challenge that corresponds to applicant's encrypted data are transmitted to the remote system; furthermore col.5, lines 56-62 disclose that hardware agent are incorporated within the remote system and local system; col.4, lines 37-65 disclose the architecture of the hardware agent which consist of having memory 43 which is a storage device such as non-volatile memory which corresponds to applicant's "storage device"), that is associated with the client (see col.5, lines 55-61 disclose that the hardware agent is associated with the remote system which corresponds to applicant's "client"; and therefore the memory 43 of hardware agent which corresponds to applicant's "storage device" in col.4, lines 58-63 also associated with the client), connected to the network (see col.1, lines 34-45 disclose medium for transmitting data back and forth between parties connected in a network environment), the client being incapable of decrypting the encrypted data (see col.3, lines 37-49 wherein it disclose that the public/private keys are stored within the hardware agent itself; col.4, lines 37-55 disclose how it is stored in order to secure the private key from being accessed; col.5, lines 1-5 disclose it can be implemented as smart cards or disk controller to automatically decrypt/ or encrypt information inputted and outputted from a hard disk; examiner considers such automatic operation with respect to decryption or encryption as corresponding to Applicant's client (remote system) incapability to decrypt the received encrypted data since no intervention on the part of the client is necessary in order to decrypt the encrypted received data. It is done automatically by the hardware agent using the pair keys stored within the memory 43),

wherein unencrypted transmission of the data through the client is bypassed (see col.5, lines 1-5 where such automatic transmission between the two hardware agent of the receiver or the transmitter system need s no intervention by the remote system which corresponds to the applicant's client and therefore the client is bypassed in that manner).

As per claims 13 and 31 Davis (6,292,892 B1) teach a method, an embedded processor program in a embedded processor-readable medium operative in a storage device that is associated with a client (see col.5, lines 55-61 disclose that the hardware agent is associated with the remote system which corresponds to applicant's "client"; and therefore the memory 43 of hardware agent which corresponds to applicant's "storage device" in col.4, lines 58-63 also associated with the client using the method of operation of the storage device for encryption and decryption purpose), of downloading data from a server in response to a client request from the client (see col.5, lines 66-67; col.6, lines 1-2 wherein the remote system which corresponds to Applicant's client sends a random challenge which corresponds to Applicant's "request from a client", the local system that corresponds to Applicant's "server" sends a response which consist of encrypted challenge which corresponds to Applicant's data back to the client. The act of sending back the response data to the client corresponds to Applicant's downloading the requested data from a server"): receiving from the server a request for downloading; receiving an encrypted data transmission from the server (see col.6, lines 2-4 wherein the hardware agent within or associated with local system encrypts the challenge that

corresponds to applicant's "encrypting the data"; col.6, lines 4-5 wherein the encrypted challenge that corresponds to applicant's encrypted data are transmitted which corresponds to applicant's "downloading" to the remote system or client; furthermore col.5, lines 56-62 disclose that hardware agent are incorporated within the remote system and local system; col.4, lines 37-65 disclose the architecture of the hardware agent which consist of having memory 43 which is a storage device such as non-volatile memory which corresponds to applicant's "storage device"); the client being incapable of decrypting the encrypted data (see col.3, lines 37-49 wherein it disclose that the public/private keys are stored within the hardware agent itself; col.4, lines 37-55 disclose how it is stored in order to secure the private key from being accessed; col.5, lines 1-5 disclose it can be implemented as smart cards or disk controller to automatically decrypt/ or encrypt information inputted and outputted from a hard disk; examiner considers such automatic operation with respect to decryption or encryption as corresponding to Applicant's client (remote system) incapability to decrypt the received encrypted data since no intervention on the part of the client is necessary in order to decrypt the encrypted received data. It is done automatically by the hardware agent using the pair keys stored within the memory 43); decrypting the encrypted data transmission to yield the data (see col.5, lines 1-5 where it disclose such hardware agent may decrypt the encrypted data in harmony with the prior steps of receiving the encrypted data); and storing the data in the storage device (see col.5, lines 1-5).

As per claims 42 and 43 Davis (6,292,892 B1) teach a storage device that is

associated with a client (col.4, lines 37-65 disclose the architecture of the hardware agent which consist of having memory 43 which is a storage device such as non-volatile memory which corresponds to applicant's "storage device"; col.5, lines 55-61 disclose that the hardware agent is associated with the remote system which corresponds to applicant's "client"; and therefore the memory 43 of hardware agent which corresponds to applicant's "storage device" in col.4, lines 58-63 also associated with the client), a data processing system for transmitting data in a network (see fig.1-3 and associated text such as col.1, lines 34-45 disclose system for transmitting data back and forth between parties connected in a network environment; col.2, lines 60-67; col.3, lines 1-9 also disclose using a computer readable medium product such as CD may employed for such transmission of data), comprising: a bus system (see col.4, lines 9-16); a processing unit connected to the bus system, wherein the processing unit includes at least one processor (see col.3, lines 54-62); memory connected to the bus system (see col.3, lines 66-67; col.4, lines 1-8); a network adapter in communication with the network and with the bus system (see col.4, lines 9-31 in harmony with col.1, lines 34-45 wherein examiner considers the Davis's gateway as corresponding to applicant's network interface for communication between the devices in a network using the bus I/O system); and a set of instructions in the memory (see col.4, lines 6-8), wherein the processing unit executes the set of instructions to perform the acts of (see col.4, lines 6-8 wherein the instruction for the host processor is for execution of them): receiving with the network adapter and from a client a request to transmit the data (see col.5, lines 66-67; col.6, lines 1-2 wherein the remote system random challenge transmission to the

local system corresponds to applicant's client request for transmitting data for authentication reasons); encrypting the data (see col.6, lines 2-4 wherein the hardware agent within or associated with local system encrypts the challenge that corresponds to applicant's "encrypting the data"); and transmitting the encrypted data to a storage device (see col.6, lines 4-5 wherein the encrypted challenge that corresponds to applicant's encrypted data are transmitted to the remote system; furthermore col.5, lines 56-62 disclose that hardware agent are incorporated within the remote system and local system; col.4, lines 37-65 disclose the architecture of the hardware agent which consist of having memory 43 which is a storage device such as non-volatile memory which corresponds to applicant's "storage device"), that is associated with a client (see col.5, lines 55-61 disclose that the hardware agent is associated with the remote system which corresponds to applicant's "client"; and therefore the memory 43 of hardware agent which corresponds to applicant's "storage device" in col.4, lines 58-63 also associated with the client), connected to the network data (see col.1, lines 34-45 disclose medium for transmitting data back and forth between parties connected in a network environment) , the client being incapable of decrypting the encrypted data (see col.3, lines 37-49 wherein it disclose that the public/private keys are stored within the hardware agent itself; col.4, lines 37-55 disclose how it is stored in order to secure the private key from being accessed; col.5, lines 1-5 disclose it can be implemented as smart cards or disk controller to automatically decrypt/ or encrypt information inputted and outputted from a hard disk; examiner considers such automatic operation with respect to decryption or encryption as corresponding to Applicant's client (remote

system) incapability to decrypt the received encrypted data since no intervention on the part of the client is necessary in order to decrypt the encrypted received data. It is done automatically by the hardware agent using the pair keys stored within the memory 43), wherein unencrypted transmission of the data through the client is bypassed (see col.5, lines 1-5 where such automatic transmission between the two hardware agent of the receiver or the transmitter system need s no intervention by the remote system which corresponds to the applicant's client and therefore the client is bypassed in that manner).

As per claims 2, 14, 20 and 32 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13, 19 and 31, further comprising: negotiating encryption parameters (see col.4, lines 48-54 disclose perform computations internally including execution of certain algorithm or protocols with respect to specific public/private key pair used for encryption and decryption. Examiner considers utilization of an algorithm, a protocol using the public/private key method as corresponding to applicant's "negotiating encryption parameters").

As per claims 3, 21 and 33 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 2, 20 and 31, wherein the step of negotiating encryption parameters includes establishing an encrypted communications channel channels (see col.4, lines 66-67; col.5, lines 1-14 disclose such encrypted parameters includes establishing encrypted channels

communication such smart cards or other peripherals or hardware agents integrated within the entity to communicate with the storage device of the target entity).

As per claims 5, 16, 23 and 35 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13, 19 and 31, wherein the data includes at least one of audio data, video data, and digital data (see col. 5, lines 66-67; col.6, lines 1-2 where it disclose data is a random challenge which is a digital data).

As per claims 6,24, 36 and 45 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13, 19 and 31, wherein the storage device stores the data in a removable medium (see col.4, lines 66-67; col.5, lines 1--3 where PCMCIA card which is a removable storage).

As per claims 7, 17, 25, 37 and 46 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13 and 31, wherein the removable medium is one of a compact disc (CD) and a digital versatile disc (DVD) (see col.2, lines 64-67 disclose a CD).

As per claims 8-9, 17, 25-26, 38-39 and 47-48 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13 and 31, teach the removable medium (see col.4, lines 66-67 and col.4, lines 1-10).

However having it as is one of a tape cartridge and a tape cassette/ or one of a holographic disc and a holographic cube is only disclose the intended use and design choice. A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The prior art is replete with references disclosing optical removable cards used to store information as applied to claims 6-7,24-25, 36-37 and 45-46 above.

As per claims 10, 18, 28, 40 and 49 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13 and 31, wherein the storage device is one of a tape drive and a disk drive (see col. 4, lines 58-63 which disclose the storage device is a non-volatile memory, that is a disk drive used to store data so upon discontinuation of power supply the information be retained).

As per claims 11, 29, 41 and 50 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13 and 31, wherein the storage device is a solid-state storage device (see col.4, lines 1-10 disclose removable storage devices. Solid-state storage by definition is a nonvolatile, removable storage medium that employs integrated circuits rather than magnetic or optical media. It is the equivalent of large-capacity, nonvolatile memory, that is integrated hardware agent having a non-volatile memory 43 in a removable storage such as PCMCIA cards). Also A recitation directed to the manner in which a claimed apparatus is intended to be

used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The prior art is replete with references disclosing optical removable cards used to store information as applied to claims 6-7,24-25, 36-37 and 45-46 above.

As per claims 12, 30 and 43 Davis (6,292,892 B1) teach the method, system and a computer program product in a computer-readable medium of claims 1, 13 and 31, wherein the storage device is independent of the client (see col.4, lines 66-67; col.5, lines 1-3 wherein the storage device may be implemented as an smart card (PCMCIA card) and therefore independent of the client system).

(11) Response to Arguments

Appellant's arguments are moot in view of new ground of rejection under U.S.C. § 102 rendered by Examiner.

Examiner has expanded the explanation on the rejection of those claims under U.S.C. § 112 second-paragraph upon appellant's request.

- Appellant's arguments with respect to rejection of the claims under U.S.C § 112 first paragraphs are not persuasive. The question is that the storage device appellant relies on is under control of the client, therefore accessible by the client. If the storage device within the client system or in association with the client system is tamper resistance even against client access such as what Davis

is teaching then, the claim language should be presented in a clear manner to reflect that. Applicant's specification page 12, lines 6-10 do disclose the party that has the key would decrypt the content. However nowhere in the claim language disclose that client has no access to a storage device, or where the public/private key pair is embedded within the associated storage which is tamper resistance in a way that encryption and decryption are done automatically and without the client intervention.

- Appellant further argues that page 7, line 11-14 depicts the operation of the secure layer (SSL) communication between the storage device and the server and where SSL relies on public key cryptography. However In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. " the operation of a SSL communication between the storage device and the server", limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
- Examiner further presents that SSL operation is well known in the art and therefore if is given as an example, it would necessitate further clarity on the claim in order for the examiner to be able to have a proper examination. As an example there is different class and subclass for exchanging keys: see using master key in class 380/281,284; using symmetric key cryptography in class 380/259; using public/private key in so many different class and subclasses. Therefore Appellant's claim language as it is written and in such broad terms with

respect to incapability of the client with respect to decryption of encrypted data within a storage device without showing how such incapability of the client is disclosed, and just refers examiner to the specification that only disclose well known art is not sufficient. If such incapability is result of using SSL, then such limitations should be present in the claim language. Why? Because then the question of the initial handshake between the two parties for exchange of the keys as Appellant has also admit in the specification is missing from the claim language, an essential step for SSL to work.

- For example the prior rejection are based on interpretation that as long as the client do not possess the decryption key, then the client has no capability, a broad but a correct interpretation by previous examiner. However the new ground of rejection is based on no accessibility of the client to the storage area where the private and public pair is embedded and where all encryption and decryption is done with no client intervention. The new ground of rejection is used to have a harmony with 112 rejections, rather than keeping the old rejections that teaches away from 112 rejections if the board would confirm it.

(12) Response to Related Proceedings Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(13) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to

reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

KAMBIZ ZAND
PRIMARY EXAMINER

Kambiz Zand

Primary Examiner

April 26, 2006

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

James L. Dwyer
DIRECTOR TC 2100

Conferees

KIM Vu (SPE AU 2134)

Justin Darrow (Primary AU 2132)

William A. Munck

P.O. Drawer 800889

Dallas, Texas 75380.

This is in response to the appeal brief filed 01/23/2006.